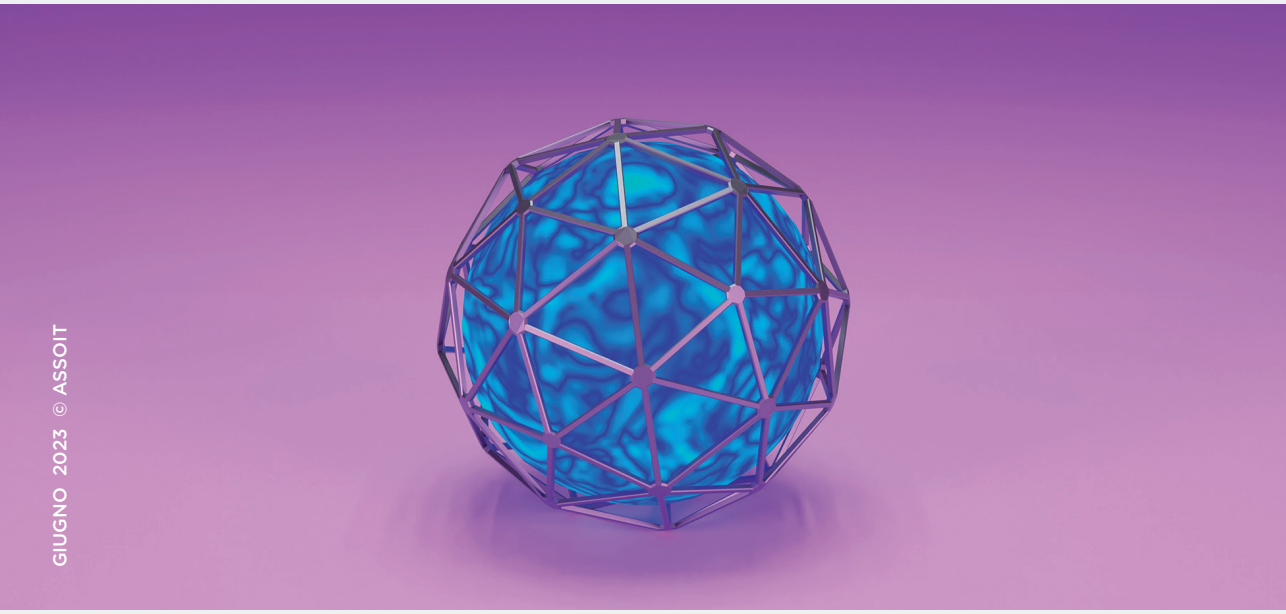
LA SICUREZZA DELLE INFORMAZIONI

Un punto imprescindibile per la protezione del dato nei sistemi di stampa, digitalizzazione e gestione documentale



ASSOIT
ASSOCIAZIONE PRODUTTORI SOLUZIONI DI STAMPA, DIGITALIZZAZIONE E GESTIONE DOCUMENTALE

LA SICUREZZA DELLE INFORMAZIONI

Un punto imprescindibile per la protezione del dato nei sistemi di stampa, digitalizzazione e gestione documentale

Versione 1.0 – GIUGNO 2023

HANNO CONTRIBUITO ALLA REALIZZAZIONE DELLA RICERCA

Brother, Canon, Epson, HP, Konica Minolta, Kyocera Document Solutions, Lexmark, Olivetti, Ricoh, Sharp, Toshiba, Xerox, Enrico Barboglio (ASSOIT), Sara Bonini (ASSOIT).

PROGETTO GRAFICO E IMPAGINAZIONE Studio Grafico Dante Cavallaro

PROGETTO E COORDINAMENTO EDITORIALE 4IT Group srl

FONTI CENTRO STUDI ASSOIT, CLUSIT ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA, QUOCIRCA

LA SICUREZZA DELLE INFORMAZIONI

Un punto imprescindibile per la protezione del dato nei sistemi di stampa, digitalizzazione e gestione documentale

SOMMARIO

ASSOIT – Il manifesto **4**

DICHIARAZIONE SULLA SICUREZZA DEI SISTEMI DI STAMPA, DIGITALIZZAZIONE E GESTIONE DOCUMENTALE **5**

INTRODUZIONE **9**

IL GDPR E L'IMPATTO SUI SISTEMI DI ACQUISIZIONE E STAMPA **11**

LE BUONE PRATICHE D'USO (BPU) **17**

MANIFESTO — LA MISSION DI ASSOIT

ASSOIT

SIAMO IL RIFERIMENTO PER LE SOLUZIONI DI STAMPA, LA DIGITALIZZAZIONE E LA GESTIONE DEI DOCUMENTI PER L'UFFICIO.

RAPPRESENTIAMO UN MERCATO DI 70.000 ADDETTI, 11 MILIONI DI DISPOSITIVI E 3 MILIARDI DI EURO DI FATTURATO.

CONDIVISIONE

DIVULGHIAMO I TREND DI MERCATO, LE NORMATIVE E LE CERTIFICAZIONI INERENTI AI SISTEMI DI STAMPA.

PROMUOVIAMO L'OTTIMIZZAZIONE DEI PROCESSI NELL'INTERA FILIERA.

INNOVAZIONE

GUIDIAMO LA TRASFORMAZIONE DELLA GESTIONE DOCUMENTALE IN UFFICIO ATTRAVERSO L'INNOVAZIONE DI DISPOSITIVI, CONSUMABILI, SOLUZIONI E SERVIZI.

INTEGRIAMO LE TECNOLOGIE DI CLOUD, INTERNET OF THINGS, MOBILITY E SECURITY.

SOSTENIBILITÀ

GARANTIAMO LA SOSTENIBILITÀ AMBIENTALE E LA QUALITÀ CERTIFICATA DEI PROCESSI DI STAMPA E GESTIONE DOCUMENTALE.

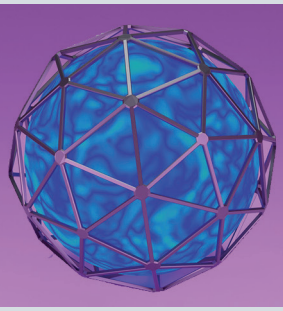
CREDIAMO NELL'ETICA COME VALORE PRIMARIO IN TUTTI I PROCESSI E SERVIZI.

LE AZIENDE ASSOCIATE

brother at your side · Canon · EPSON · hp · KONICA MINOLTA · KYOCERA · Lexmark · OKI · Olivetti · RICOH imagine. change. · SHARP · TOSHIBA · xerox

SEGRETERIA ORGANIZZATIVA 4IT group

DICHIARAZIONE SULLA SICUREZZA DEI SISTEMI DI STAMPA, DIGITALIZZAZIONE E GESTIONE DOCUMENTALE



ASSOIT

ASSOCIAZIONE PRODUTTORI SOLUZIONI DI STAMPA, DIGITALIZZAZIONE E GESTIONE DOCUMENTALE

DICHIARAZIONE SULLA SICUREZZA DEI SISTEMI DI STAMPA, DIGITALIZZAZIONE E GESTIONE DOCUMENTALE

Negli ultimi anni gli attacchi informatici compiuti ai danni di aziende private e pubbliche amministrazioni sono aumentati esponenzialmente diventando sempre più subdoli e sofisticati.
Secondo il rapporto del CLUSIT, l'Associazione Italiana per la Sicurezza Informatica, **nel primo semestre del 2022 sono stati registrati 1.141 attacchi, numero che rappresenta una crescita del +53% rispetto allo stesso periodo dello scorso anno.**

Il nostro è il quarto Paese più colpito al mondo.

A questo dato, già allarmante, si sono aggiunti nel tempo diversi scenari di guerra, che si stanno combattendo anche sul fronte digitale. Sono conflitti allargati, che coinvolgono anche gruppi associati alla criminalità organizzata.

La salvaguardia delle informazioni è un punto imprescindibile nelle attività delle piccole e medie imprese, il tessuto produttivo del nostro Paese. Purtroppo, però, questa consapevolezza è ancora troppo poco radicata e le conseguenze di questa condizione sono gli attacchi costanti, perpetrati ogni giorno a queste realtà.
Un ulteriore punto debole è rappresentato dalla mancanza di comprensione e conoscenza delle norme e delle minacce relative alla sicurezza, nonostante l'introduzione di regolamenti e standard sempre più stringenti e punitivi (GDPR).
Le case produttrici di sistemi di stampa, digitalizzazione e gestione documentale presenti in Italia, associate ad ASSOIT, sono pienamente consapevoli delle potenziali minacce e attacchi ai dispositivi da essi prodotti. Se questi non sono gestiti correttamente possono rappresentare un potenziale punto debole in rete e nelle policy aziendali di sicurezza dei dati.

Tutti i produttori associati ad ASSOIT hanno dotato i loro sistemi di stampa con funzionalità che garantiscono la protezione delle informazioni, come l'autenticazione e l'autorizzazione per

verificare l'identità degli utenti prima che venga rilasciata qualsiasi stampa. I metodi di convalida possono essere diversi: lettori badge, codici PIN o sistemi di autenticazione biometrica.

La sicurezza viene applicata a 360°: hardware e software, applicazioni, sistema operativo, firmware, bios e disco fisso; questo per assicurare che i processi di gestione dei documenti e delle stampe siano conformi alle più stringenti normative.

Ogni elemento è crittografabile in modo che i dati, se carpiti, siano resi illeggibili e inutilizzabili.
Inoltre, le case produttrici rilasciano regolarmente aggiornamenti per la sicurezza dei sistemi anche per essere protetti da tentativi di installazione di applicazioni o software malevoli.
L'intero processo è salvaguardato, anche in fase di digitalizzazione e di gestione documentale. Questi sistemi sono monitorabili da remoto, con cruscotti in grado di rilevare e allertare i responsabili della sicurezza relativamente ad accessi non autorizzati, in modo da permettere un tempestivo intervento proattivo.
Infine, un ulteriore aspetto che non va trascurato è quello relativo alla sensibilizzazione degli utenti: spesso gli incidenti relativi alla sicurezza delle informazioni accadono perché non è stata adottata una politica di informazione precisa e puntuale sui rischi e sulle potenziali minacce.

Le case produttrici lavorano costantemente, con la comunità dei partner e dei rivenditori, per implementare procedure, assicurare formazione e consulenza per la protezione e la sicurezza dei sistemi di stampa, digitalizzazione e gestione documentale presenti nelle aziende, nelle istituzioni e nelle case dei privati cittadini.

INTRODUZIONE

PER LA SICUREZZA DEI SISTEMI DI STAMPA, LA SFIDA È DOPPIA: "FISICA" E DIGITALE.

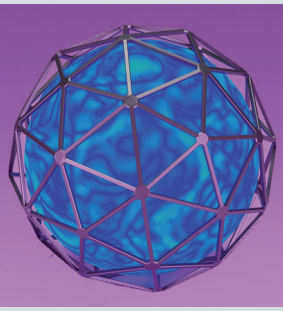
Cosa intendiamo per "fisica"? Quante volte avete visto abbandonato su una stampante un documento contenente informazioni riservate? Il vassoio di uscita rappresenta il posto più comune dove trovare documenti con informazioni sensibili e riservate che possono cadere in mani sbagliate.
È bene quindi proteggere le informazioni impostando un sistema di autenticazione che ne sblocchi la stampa.

I sistemi di stampa e digitalizzazione sono dei dispositivi IoT, fanno parte delle reti aziendali e degli strumenti IT, in grado di memorizzare elevate quantità di dati sui loro dischi fissi. Sono accessibili da dispositivi mobili e dal cloud e possono rappresentare, come altri strumenti, se non correttamente protetti, un punto di ingresso per attacchi da parte di cyber criminali.

Le stampanti e i dispositivi di nuova generazione contengono firmware, processori, dischi rigidi con capacità di connessione elevate esattamente come un notebook, ma spesso trascuriamo le stampanti perché non interagiamo direttamente con loro, non a caso, vengono definite "periferiche" dove stampare o digitalizzare fatture, informazioni riservate, dati.

La connessione tra i notebook o i PC e le stampanti funziona in modo bidirezionale, può essere sfruttata per diffondere malware, ransomware che rendono inaccessibili i file, chiedendo il pagamento di un riscatto per ripristinarli. Questo è uno dei molteplici attacchi che una stampante può subire. In questa ricerca, redatta dai produttori di soluzioni di stampa, digitalizzazione e gestione documentale associati ad **ASSOIT**, vengono approfonditi i rischi legati alla non conformità con le normative sulla protezione dei dati, l'approccio alla sicurezza, le buone pratiche d'uso.

IL GDPR E L'IMPATTO SUI SISTEMI DI ACQUISIZIONE E STAMPA



ASSOIT
ASSOCIAZIONE PRODUTTORI SOLUZIONI DI STAMPA, DIGITALIZZAZIONE E GESTIONE DOCUMENTALE

IL GDPR E L'IMPATTO SUI SISTEMI DI ACQUISIZIONE E STAMPA

Il General Data Protection Regulation (meglio conosciuto con il suo acronimo "GDPR") è il Regolamento (UE) 2016/679 che ha modificato e uniformato a livello europeo la normativa privacy.

Entrato in vigore il 24 maggio 2016, è diventato applicabile e vincolante in tutti i Paesi europei a decorrere dal 25 maggio 2018. Il GDPR rappresenta un traguardo importantissimo per la tutela del dato personale, nel contesto di una rapida evoluzione tecnologica e lo pone al centro del business delle imprese che impone di armonizzare le regole con cui questo dato è trattato.

L'obiettivo di questo Regolamento è principalmente quello di tutelare e rafforzare i diritti dei soggetti interessati, creando regole uniformi tra i Paesi membri. Si tratta di un cambio epocale che richiede necessariamente una gestione della privacy che vada ben oltre la creazione di policy, permeando i processi aziendali.

Il diritto alla protezione dei dati personali è garantito dall'Art. 5 GDPR (Principi sul trattamento dei dati personali). Da esso deriva per le aziende l'obbligo sia di documentare in modo esteso i sistemi di raccolta e conservazione dei dati sia di riportare la perdita di dati in modo tempestivo.
Eventuali violazioni sono multate con importi molto alti.

L'articolo 83 del Regolamento UE prevede sanzioni fino a:

10 milioni di euro o 2% del fatturato mondiale nei casi in cui, per esempio, i dati personali degli utenti vengano trattati in maniera illecita, non venga nominato il DPO, non venga comunicato un data breach all'Autorità Garante;

20 milioni di euro o 4% del fatturato nei casi più gravi, come ad esempio l'inosservanza dei diritti degli interessati o il trasferimento illecito di dati personali ad altri Paesi.

LE SCELTE DA EFFETTUARE

FOCUS

Le aziende sono chiamate a rispettare la normativa, ma devono anche dimostrare che i loro processi siano conformi, documentando in modo adeguato le decisioni intraprese per proteggere i dati personali.
La normativa definisce i dati personali come "ogni informazione che riguarda indicazioni personali o materiali relative a un individuo identificato o identificabile con precisione".

È evidente che tutta l'infrastruttura IT di una azienda o di una pubblica amministrazione viene coinvolta per essere adattata e resa conforme a queste nuove normative. Un punto solitamente poco considerato è la protezione dei dati nei processi di stampa. In fondo, i data leak non sono per forza i cyber attacchi, ma possono essere qualcosa di molto più semplice, come documenti che escono dalle stampanti e finiscono in mani sbagliate.

Molto spesso si sottovaluta che esistono rischi di sicurezza significativi, per quanto riguarda i dati personali, anche durante i processi di stampa:

- la trasmissione in chiaro di dati personali all'interno di un network;
- la conservazione in chiaro di dati personali sui server o sui dischi fissi di una stampante;
- l'invio di documenti confidenziali sulle stampanti sbagliate;
- la possibilità che documenti che contengono dati personali finiscano nelle mani sbagliate,

Molte aziende possono non essere al corrente che i dati personali vengono trasferiti in modo visibile, e non cifrato, sulla rete, per essere stampati. Oppure vengono salvati in chiaro sui server, o addirittura sui dischi delle stampanti.

LA POSIZIONE ASSOIT

ASSOIT suggerisce di lavorare sui processi di workflow per evitare che informazioni sensibili possano finire nelle mani sbagliate e sulla implementazione di funzioni di stampa mediante sistema di riconoscimento dell'utente, per evitare che un documento resti dimenticato nel vassoio di uscita di una stampante.

La sicurezza di stampa deve diventare parte fondamentale dei processi di pianificazione IT delle aziende. E per fare ciò, le aziende stesse devono considerare le aree principali della sicurezza di stampa.

La prima è rappresentata dai dispositivi. Molte organizzazioni hanno in casa dispositivi di stampa vecchi e protetti in modo inadeguato.

Sostituire un parco composto da dispositivi vecchi ed obsoleti con device di ultima generazione è il primo passo verso la messa in sicurezza della propria flotta dI dispositivi di stampa.
Implementare successivamente funzioni di accesso sicuro che riservino la possibilità di usare i dispositivi di stampa a soggetti specifici, facendo uso di strumenti predefiniti di controllo di accesso degli utenti, fornisce all'azienda un secondo layer di sicurezza dal punto di vista dell'accesso al dispositivo ed ai documenti da esso stampati.

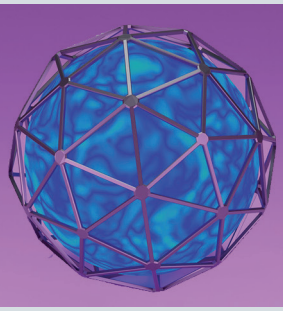
La seconda area è la rete. Con l'uso sempre più marcato di dispositivi mobili e la necessità di supportare iniziative BYOD, i dipartimenti IT devono trovare un equilibrio ideale tra la possibilità di fornire agli utenti gli strumenti necessari a massimizzare l'efficienza, e al tempo stesso la necessità di ridurre al minimo i rischi di intrusione attraverso reti e connessioni. Questo può includere certificati digitali, port filtering, IP address filtering, controllo degli accessi basato su ruoli, e molto altro ancora.

La terza area è rappresentata dai documenti. Una stampa non sicura può essere evitata sul dispositivo, configurandolo in modo da consentire lavori di stampa solo se l'utente si autentica.
È anche possibile implementare un'autenticazione via badge per l'accesso ai locali fisici, l'uso di soluzioni di rilascio della stampa e un monitoraggio sicuro dei documenti. Si tratta di opzioni che permettono grande visibilità sui documenti fisici e riducono sensibilmente i rischi legati a minacce interne.

Infine, i dati. Assicurarsi che i job di stampa viaggino sulla rete aziendale o in cloud in modalità cifrata consente all'azienda di evitare pericolosi e deleteri data breach di cui sempre più spesso troviamo traccia sui media. Data breach che possono portare ad ingenti danni economici e ad incalcolabili danni alla reputazione dell'azienda coinvolta.

Alla fine, è fondamentale che le aziende inizino a considerare la sicurezza come una componente integrale del loro hardware di stampa, e non solo dell'infrastruttura software e IT, assicurando che la loro conformità alle norme di protezione dei dati si estenda lungo l'intero percorso che va dalla sicurezza web fino al cassetto di uscita della stampante.

LE BUONE PRATICHE D'USO



ASSOIT

ASSOCIAZIONE PRODUTTORI SOLUZIONI DI STAMPA, DIGITALIZZAZIONE E GESTIONE DOCUMENTALE

BUONE PRATICHE D'USO

Aggiornamento dei dispositivi

È utile prendere in considerazione l'aggiornamento del proprio parco stampanti. Molte nuove stampanti dispongono di funzionalità di sicurezza integrate che semplificano la protezione della rete e la protezione da un attacco informatico.

Mantenere aggiornato il software dei dispositivi

Le stampanti hanno spesso un firmware che le aiuta a funzionare, potrebbero anche avere un software antivirus o anti-malware integrato. È bene consultare il manuale del proprio dispositivo per conoscere le diverse caratteristiche e la sua manutenzione. È inoltre importante installare eventuali patch di sicurezza o aggiornamenti, poiché il software obsoleto è spesso una delle cause principali che porta alla violazione dei dati.

Creare policy aziendali per proteggere i dati contenuti negli hard disk e sui documenti lasciati nei vassoi delle stampanti

Creare una serie di regole pratiche e norme di condotta sono la base per ottenere una linea di difesa verso gli attacchi. Una serie di policy adeguate può aiutare a proteggere sistemi e utenti, anche coloro che lavorano in remoto.

Mettere in atto un processo di autenticazione

Una buona pratica è quella di verificare che le stampanti dispongano di misure di sicurezza come pass code univoci per trattenere le stampe fino a quando un utente non è fisicamente presente per ritirarli. Questo processo permette di verificare i dati inviati, per questo le stampanti potrebbero subire altre vulnerabilità che potrebbero rivelarsi sfruttabili, anche da remoto I sistemi di stampa e digitalizzazione sono dotati di funzionalità che garantiscono la protezione delle informazioni, come l'autenticazione e l'autorizzazione per verificare l'identità degli utenti prima che venga rilasciata qualsiasi stampa. I metodi di convalida possono essere diversi: lettori badge, codici PIN o sistemi di autenticazione biometrica.

Utilizzare i software di monitoraggio

Il software di monitoraggio dei dispositivi di stampa permette di avere sotto controllo tutte le attività di stampa della propria organizzazione. Questi cruscotti sono inoltre in grado di individuare attività sospette e consentire una reazione tempestiva agli attacchi.
Gli utenti dei servizi di stampa gestiti (MPS) possono anche ottenere regolari report di conformità, che dovrebbero includere il monitoraggio e la segnalazione delle violazioni dei dati.

Posizionare i dispositivi di stampa e digitalizzazione su una rete separata e dedicata all'interno dello spazio di lavoro

Posizionare le stampanti su una rete separata non eliminerà la minaccia di malintenzionati che accedono alla rete aziendale da questi dispositivi, ma impedirà loro di utilizzarli come potenziali punto di ingresso nella rete aziendale.

Formare e rendere consapevoli gli utenti su minacce e attacchi

Questa pratica consente di rendere informati gli utenti sui rischi legati ai dispositivi di stampa. Sensibilizzare gli utenti dotandoli di regole di comportamento è il primo passo verso una maggiore sicurezza. Una survey contenuta nel Rapporto Clusit 2023 sulla Sicurezza ICT in Italia, ha evidenziato che le policy e le procedure di sicurezza pubblicate sono conosciute da dipendenti e collaboratori solo in un terzo (33%) delle aziende.

Sanificazione dei dati al momento della sostituzione dei dispositivi

È importante accertarsi che il dispositivo sia sottoposto ad un procedimento di sanificazione certificata dei dati che include la distruzione degli hard disk, o la loro formattazione in modalità sicura a basso livello, e la cancellazione di tutti i dati presenti nelle rubriche interne al dispositivo, come per esempio rubrica e-mail, rubrica telefonica-fax, al momento della sua sostituzione. Questa pratica consente di distruggere in modo definitivo tutti i dati contenuti in questi dispositivi e la certificazione, dichiarazione emessa dal fornitore che effettua il servizio, tutela l'azienda o il privato che ha utilizzato il dispositivo fino a quel momento.

Servizi professionali di Print Security Risk Assessment

Come già detto, spesso il perimetro dei dispositivi di stampa non viene tenuto nella giusta considerazione da parte del personale IT, che tende a valutare come sicuro un ambiente nel quale invece i potenziali bug di sicurezza sono presenti. È raccomandato valutare col proprio fornitore di dispositivi di stampa la possibilità di usufruire di un servizio professionale di Security Risk Assessment per i dispositivi di stampa grazie al quale verranno analizzate in profondità tutte le potenziali aree di rischio: hardware, firmware, network, processi e procedure, asset management, configurazioni iniziali e manutenzione delle stesse, patching, governance.

Buone pratiche a casa

Avere una stampante non protetta collegata alla rete domestica o aziendale è come lasciare una porta aperta nella propria stanza o in ufficio. Quindi, è bene assicurarsi di rivedere e disabilitare tutto ciò che comporta la stampa su Internet. Ciò include la configurazione delle impostazioni di rete in modo che la stampante risponda solo ai comandi provenienti dal router di rete. Inoltre, non dimenticare di scollegare la stampante quando non è in uso: se non c'è connessione, i malintenzionati non possono compromettere la rete.

LA SICUREZZA DELLE INFORMAZIONI

Un punto imprescindibile per la protezione del dato nei sistemi di stampa, digitalizzazione e gestione documentale

LA RICERCA È DISPONIBILE SU **WWW.ASSOIT.IT**

ASSOIT
ASSOCIAZIONE PRODUTTORI SOLUZIONI DI STAMPA, DIGITALIZZAZIONE E GESTIONE DOCUMENTALE